IN THE CLAIMS

Please cancel claims 1 – 5 and 28 - 30. Please add claims 32 and 33. and amend claims 8, 16, 22, 24, 25, and 27 as follows.

~~Claims 1 – 5 (cancelled).~~

6. (cancelled)

7. (cancelled).

~~8. (currently amended) A computing system for performing a decryption~~ operation on an encrypted packet, comprising:

a network driver to regulate said decryption operation and to transmit a decryption command;

~~a controller to perform said decryption operation;~~

a host memory ~~to store data that is used or generated by said decryption operation~~ to store the encrypted packet after receipt by the computing system;

a controller to perform said decryption operation after receiving said decryption command from the network driver;

a network interface to specify[[ing]] an average ~~latency value to the controller~~;

a bus providing electronic communication among said network driver, said host memory and said controller, ~~said decryption operation converting said encrypted packed into a decrypted packet, and~~ said controller asserting an interrupt prior to a complete transfer of said decrypted packet from said controller to said host memory, wherein the controller waits the average latency value before said assertion of the interrupt in response to said decryption command ~~and said controller asserts an additional interrupt after completion of said decryption operation and said network driver specifies an~~

~~average latency value to said controller for use in said decryption operation~~.

9. (original) The computing system of claim 8, wherein said computer further includes a network interface to provide electronic communication between said computer and a network.

10. (original) The computing system of claim 9, wherein at least one security association (SA) is stored in said host memory.

11. (previously presented) The computing system of claim 10, wherein said network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said controller to transfer said encrypted packet and said one SA across said bus to said controller.

12. (original) The computing system of claim 8, wherein said network interface includes a cryptography accelerator.

13. (original) The computing system of claim 8, wherein said controller transfers said decrypted packet across said bus from said controller to said host memory.

14. ~~(cancelled)~~

15. (cancelled).

16. (currently amended) A method of decrypting an encrypted packet received by a computing system, comprising:

receiving said encrypted packet from a network and transferring said encrypted packet to a host memory;

~~issuing a decryption command to a controller;~~

specifying an average latency value to the controller;

~~determining a time for~~ waiting the average latency value before said assertion of

[[said]] an interrupt in response to said decryption command;

transferring said encrypted packet to said controller;

converting said encrypted packet to a decrypted packet; and

transferring said decrypted packet to [[a]] the host memory; wherein ~~asserting an~~ the interrupt is asserted at a time before completing said transfer of said decrypted packet to said host memory[[, and]]

~~asserting an additional interrupt upon completion of said transfer of said decrypted packet to said host memory~~.

~~17.~~ (cancelled)

18. (original) The method of claim 16, wherein said step of converting said encrypted packet to said decrypted packet further includes:

~~parsing said encrypted packet;~~

matching said encrypted packet with a corresponding security association (SA) stored in said host memory; and

~~transferring said encrypted packet and said corresponding SA to a controller.~~

19. (original) The method of claim 16, wherein said step of converting said encrypted packet to said decrypted packet further includes authenticating said decrypted packet.

20. (cancelled).

21. (original) The method of claim 16, further including indicating said decrypted packet to a protocol stack ~~after asserting said interrupt~~.

22. (currently amended) A program code storage device, comprising:

a machine-readable storage medium; and

machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions that when executed cause ~~the device~~ a computer system to:

receive said encrypted packet from a network and transfer said encrypted packet to a host memory;

~~issue a decryption command to a controller;~~

specify an average latency value to the controller;

~~determine a time for~~ waiting the average latency value before said assertion of [[said]] an interrupt in response to said decryption command;

transfer said encrypted packet to said controller;

convert said encrypted packet to a decrypted packet; and

~~transfer said decrypted packet to~~ [[a]] the ~~host memory[[; and]]~~ , wherein ~~assert an interrupt~~ the interrupt is asserted at a time before completing said transfer of said decrypted packet to said host memory; ~~and~~

~~assert an additional interrupt upon completion of said transfer of said decrypted packet to said host memory~~.

23. (cancelled)

24. ~~(currently amended)~~ The device of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet ~~further~~ includes instructions to:

parse said encrypted packet;

~~match said encrypted packet with a corresponding security association (SA)~~ stored in said host memory; and

transfer said encrypted packet and said corresponding SA to a controller.

25. (currently amended) The device of claim 22, wherein said instructions to convert said encrypted packet to said decrypted packet ~~further~~ includes instructions to authenticate said decrypted packet.

26. (cancelled)

27. (currently amended) The device of claim 22, ~~further~~ including instructions, which when executed cause the computing system to indicate said decrypted packet to a protocol stack after the instruction to assert said interrupt.

Claims 28 – 30 (cancelled).

31. (cancelled).

32. (new) The method of claim 16, further including asserting the interrupt before the encrypted packet is fully decrypted.

33. (new) The program code storage device of claim 22, including instructions which when executed the device to assert the interrupt before the encrypted packet is fully decrypted.